4. REPRISE ON EQUIVALENCE RELATIONS

Firstly we recall:

Definition 107 *A (binary)* ***relation*** $\sim$ *on a set* S *is a subset of* $S \times S$.

Then, for $a, b, \in S$, *we write* $a \sim b$ *if and only if* $(a, b) \in S$.

We might just as easily view the relation as a function $\sim\colon S \times S \to \{T, F\}$, *that is a function with two inputs from* S *and output True* (T) *or False* (F). *The "set"* $\sim$ *would then be* $\sim^{-1}(T)$.

Example 108 *(i) With* $S = \mathbb{Z}$, *we would have "*$\leqslant (3,4) = T$*" or "*$(3,4) \in \leqslant$*" as rather unnatural ways of simply saying "*$3 \leqslant 4$*".*
(ii) If $S = \{1, 2, 3\}$ *then* $<$ *is the set* $\{(1,2), (1,3), (2,3)\}$.

Definition 109 *We say that a relation* $\sim$ *on a set* S *is an equivalence relation if it is*
(i) ***reflexive*** *– that is* $a \sim a$ *for all* $a \in S$;
(ii) ***symmetric*** *– that is, whenever* $a \sim b$ *then* $b \sim a$;
(iii) ***transitive*** *– that is, whenever* $a \sim b$ *and* $b \sim c$ *then* $a \sim c$.

Example 110 *The following are all examples of equivalence relations:*
(i) $S = \mathbb{C}$ *with* $z \sim w$ *iff* $|z| = |w|$;
(ii) $S = GL(n, \mathbb{R})$ *with* $A \sim B$ *iff there exists* $P \in GL(n, \mathbb{R})$ *such that* $A = P^{-1}AP$;
(iii) $S = \{$*polygons in* $\mathbb{R}^2\}$ *and* $\sim$ *is congruence;*
(iv) $S = \mathcal{P}(X)$ *and* $A \sim B$ *if* $|A| = |B|$;
(v) S *is a group and* $x \sim y$ *if* $x = y$ *or* $x = y^{-1}$;
(vi) $S = C^1(\mathbb{R})$ *with* $f(x) \sim g(x)$ *if* $f'(x) = g'(x)$.

Example 111 *The following relations* ***aren't*** *equivalence relations:*
(i) $S = \mathbb{Z}$ *with* $m \sim n$ *iff* $m < n$ *as* $\sim$ *isn't reflexive or symmetric;*
(ii) $S = \mathcal{P}(X)$ *with* $A \sim B$ *iff* $A \subseteq B$ *as* $\sim$ *isn't symmetric;*
(iii) $S = \mathbb{R}[x]$ *with* $p(x) \sim q(x)$ *iff* $p(a) = q(a)$ *for some* $a \in \mathbb{R}$ *as* $\sim$ *isn't transitive.*

Proposition 112 *Let* $S = \mathbb{Z}$ *and* $n \geqslant 2$ *is an integer. If we set* $a \sim b$ *if* $a - b$ *is a multiple of* n *then* $\sim$ *is an equivalence relation.*

Proof. (a) For any $a \in \mathbb{Z}$ we have $a \sim a$ as 0 is a multiple of n.
(b) If $a \sim b$ then $a - b = kn$ for some integer k. Then $b - a = -kn$ and hence $b \sim a$.
(c) If $a \sim b$ and $b \sim c$ then $a - b = kn$ and $b - c = ln$ for integers k, l. But then

$$a - c = (a - b) + (b - c) = (k + l)n$$

and hence $a \sim c$. ■

Definition 113 *Let G be a group and $g, h \in G$. Then g and h are said to be* ***conjugate in*** *G if there exists $k \in G$ such that $g = k^{-1}hk$. (Compare with Definition 71.)*

Proposition 114 *Conjugacy is an equivalence relation.*

Proof. Let G be a group and write $g \sim h$ if there exists k such that $g = k^{-1}hk$. Then:
(a) $\sim$ is reflexive as $g = e^{-1}ge$ for all g.
(b) If $g = k^{-1}hk$ then $h = kgk^{-1} = (k^{-1})^{-1} gk^{-1}$ and hence $\sim$ is symmetric.
(c) If $g_1 \sim g_2$ and $g_2 \sim g_3$ then there exist k_1 and k_2 such that

$$g_1 = k_1^{-1} g_2 k_1 \qquad \text{and} \qquad g_2 = k_2^{-1} g_3 k_2.$$

Hence $g_1 = k_1^{-1}k_2^{-1}g_3k_2k_1 = (k_2k_1)^{-1} g_3 (k_1k_2)$. ■

Definition 115 *Given an equivalence relation $\sim$ on a set S with $a \in S$, then the* ***equivalence class of*** *a, written $\bar{a}$ or $[a]$, is the set*

$$\bar{a} = \{x \in S : x \sim a\}.$$

Example 116 *Given the equivalence relation in Proposition 112 there are n equivalence classes namely $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$. This follows from the division algorithm in $\mathbb{Z}$. We see that*

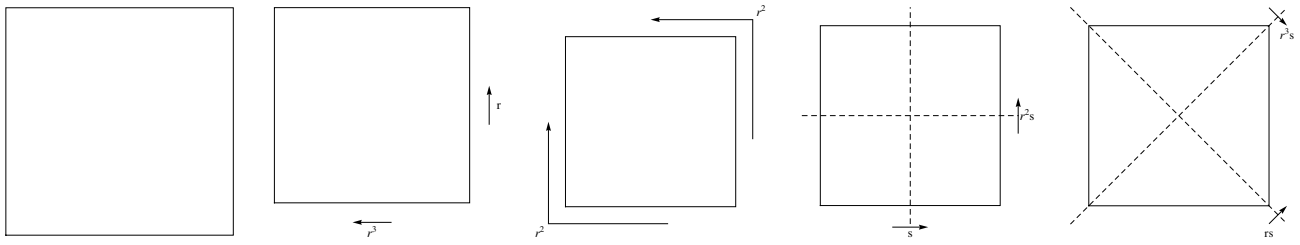
$$\bar{0} = n\mathbb{Z}; \qquad \bar{1} = 1 + n\mathbb{Z}; \qquad \ldots \qquad \overline{n-1} = (n-1) + n\mathbb{Z} = -1 + n\mathbb{Z}.$$

Example 117 *The conjugacy class of σ in S_n are those permutations of the same cycle type.*

Example 118 *The conjugacy classes of D_8 are*

$$\{e\}, \quad \{r, r^3\}, \quad \{r^2\}, \quad \{s, r^2s\}, \quad \{rs, r^3s\}.$$

Diagrammatically it is a little clearer as to what is going on

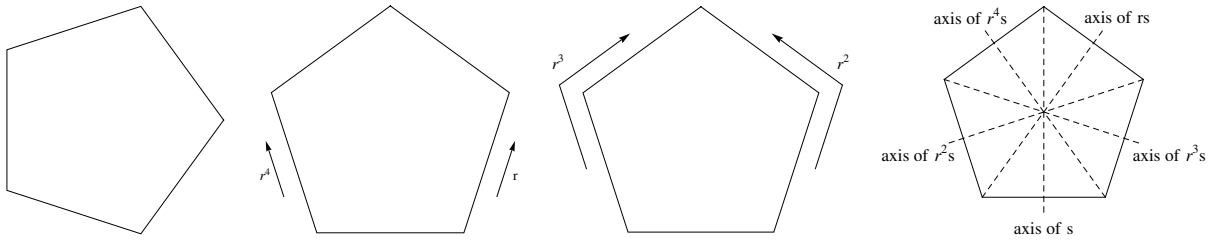


Depending on their viewpoints, two observers might confuse reflection in the horizontal with it in the vertical, but will be certain that the square wasn't reflected in a diagonal; likewise they might conflate rotation by a right angle anticlockwise with the same in a clockwise fashion.

For D_{10} the conjugacy classes are

$$\{e\}, \quad \{r, r^4\}, \quad \{r^2, r^3\}, \quad \{s, rs, r^2s, r^3s, r^4s\}.$$

Again, diagrammatically, it is a little clearer as to what is going on



The general cases are investigated in Exercise Sheet 5, Question 3.

Definition 119 *Let S be a set and Λ be an indexing set. We say that a collection of subsets A_λ of S (where $\lambda \in \Lambda$) is a partition of S if*

(i) $A_\lambda \neq \varnothing$ for each $\lambda \in \Lambda$;

(ii) $\bigcup_{\lambda\in\Lambda} A_\lambda = S$;

(iii) if $\lambda \neq \mu$ then $A_\lambda \cap A_\mu = \varnothing$, or equivalently: if $A_\lambda \cap A_\mu \neq \varnothing$ then $\lambda = \mu$.

Notation 120 *Given a partition P of S and $a \in S$, we will write P_a for the unique set in P such that $a \in P_a$.*

Theorem 121 *Let $\sim$ be an equivalence relation on a set S. Then the $\sim$-equivalence classes partition S.*

Proof. Firstly, $a \in \bar{a}$ for any $a \in S$ by reflexivity; this shows that equivalence classes are non-empty and also that their union is S. Secondly, we need to show that distinct equivalence classes are disjoint. So suppose that $c \in \bar{a} \cap \bar{b}$ for $a, b, c \in S$. We need to show that $\bar{a} = \bar{b}$. As $c \in \bar{a}$ then $c \sim a$ and likewise $c \sim b$. By symmetry and transitivity it follows that $a \sim b$. So if $x \in \bar{a}$ we have $x \sim a \sim b$ and hence, by transitivity, $x \sim b$. We have shown that $\bar{a} \subseteq \bar{b}$. If we swap the roles of a and b in the above argument then $\bar{b} \subseteq \bar{a}$ and the result follows. ■

Theorem 122 *Let S be a set.*

(a) Given an equivalence relation $\sim$ on S then the equivalence classes of $\sim$ form a partition $P(\sim)$ of S (where $P(\sim)_a = \bar{a}$ for each $a \in S$).

(b) Given a partition P of S then the relation $\sim_P$ on S defined by

$$a \sim_P b \text{ if and only if } b \in P_a$$

is an equivalence relation on S.

(c) As given above, (a) and (b) are inverses of one another; that is

$$P(\sim_P) = P \qquad \text{and} \qquad \sim_{P(\sim)} = \sim .$$

In particular, there are as many equivalence relations on a set S as there are partitions of the set S.

Proof. (a) was proven in the previous theorem. To prove (b), suppose that P is a partition of S.

- Let $a \in S$. Then $a \in P_a$ by definition and so $a \sim_P a$.
- If $a \sim_P b$ then $b \in P_a$ and $b \in P_b$ by definition. So $b \in P_a \cap P_b \neq \varnothing$ and hence $P_a = P_b$. Thus $b \in P_a$.
- If $a \sim_P b$ and $b \sim_p c$ then $b \in P_a$ and $c \in P_b$. As $b \in P_a \cap P_b \neq \varnothing$ then $P_a = P_b$ and so $c \in P_a$ and $a \sim_P c$.

(c) Let P be a partition of S.

$$\begin{aligned} A \in P(\sim_P) &\iff \text{there is } a \in A \text{ such that } A \text{ is the } \sim_P\text{-equivalence class of } a \\ &\iff \text{there is } a \in A \text{ such that } A = P_a \\ &\iff A \in P. \end{aligned}$$

Likewise

$$a \sim_{P(\sim)} b \iff b \in (P(\sim))_a \iff a \in \bar{b} \iff a \sim b$$

■

Example 123 *There are* 52 *equivalence classes on a set with* 5 *elements.*

Solution. Let $X = \{1, 2, 3, 4, 5\}$. As the only ways to partition the integer 5 is

$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1$$

and for each such possibility there correspond the following partitions of X

Partition of 4	Partitions of X
5	1
$4+1$	$\binom{5}{1} = 5$
$3+2$	$\binom{5}{2} = 10$
$3+1+1$	$\binom{5}{3} = 10$
$2+2+1$	$\frac{1}{2!}\binom{5}{2}\binom{3}{2} = 15$
$2+1+1+1$	$\binom{5}{2} = 10$
$1+1+1+1+1$	1

■

Example 124 *How many partitions are there of a set with* 22 *elements into* 3 *subsets of size* 4 *and* 2 *subsets of size* 5*?*

Solution. The answer is 1254751898400 counted either of the following ways:

$$\frac{\overbrace{\binom{22}{3}\binom{19}{3}\binom{16}{3}\binom{13}{3}\binom{10}{5}\binom{5}{5}}^{\text{ways of filling the six sets}}}{\underbrace{4!2!}_{\text{shuffling same-size subsets}}} = \frac{\overbrace{22!}^{\text{ways of placing the 22 elements}}}{\underbrace{(3!)^4\,(5!)^2}_{\text{shuffling within subsets}} \times \underbrace{4!2!}_{\text{shuffling same-size subsets}}}.$$

■

4.1 Modular Arithmetic

Consider the odd and even integers. The product of two odd integers is an odd integer, no matter what odd integers we have in mind. Likewise we can see, for example, that

$$\text{Even} \times \text{Odd} = \text{Even}, \qquad \text{Odd} + \text{Odd} = \text{Even},$$

again irrespective of the even and odd numbers we have in mind. If we fill out the addition and multiplication tables for {Even, Odd} then we obtain

$+$	Even	Odd
Even	Even	Odd
Odd	Odd	Even

,

$\times$	Even	Odd
Even	Even	Even
Odd	Even	Odd

.

You may notice that {Even, Odd} under + makes an abelian group with Even being the additive identity. In fact, more than that, {Even, Odd} under + and × make a commutative ring with identity Odd.

More properly the above tables describe the arithmetic of the integers "modulo 2" or more simply "mod 2". **Modular arithmetic** is the study of remainders. If we divide an integer by 2 then there are two possible remainders 0 (when the integer is even) and 1 (when the integer is odd). We could instead rewrite the above addition and multiplication with 0 replacing Even and 1 replacing Odd. The tables would then look like:

$+$	0	1
0	0	1
1	1	0

,

$\times$	0	1
0	0	0
1	0	1

.

Most of those calculations look fairly natural with the exception of $1 + 1 = 0$, but recall the equation is really conveying that an odd number added to an odd number makes an even number. From the point of view of remainders, adding the two remainders of 1 makes a whole new factor of 2; these two 1s add to *clock* back to 0.

In fact, modular arithmetic is sometimes also referred to as **clockwork arithmetic** and another everyday example of modular arithmetic is the 12-hour clock. It would not be at all surprising for me to say that 5 hours after 9 o'clock comes 2 o'clock or that 7 hours before 1 o'clock was 6 o'clock or that 7 three-hour shifts that started at 2 o'clock will end at 11 o'clock. In mod 12 arithmetic we would write these calculations as

$$5 + 9 = 2, \qquad 1 - 7 = 6, \qquad 2 + 7 \times 3 = 11.$$

These facts are true irrespective of what day of the week we are discussing or whether 5 represents 5am or 5pm.(The only significant difference between mod 12 arithmetic and the 12-hour clock is that we write 0, instead of 12, for noon and midnight.)

More generally, we can use the division algorithm to describe the possible remainders when we divide by any integer $n \geqslant 2$.

Definition 125 *If we are doing arithmetic* mod n*, (where* $n \geqslant 2$*) then, by the division algorithm in* $\mathbb{Z}$*, there are* n *possible remainders, namely*

$$0, 1, 2, 3, \ldots, n-1.$$

We define here rules for how to add, subtract and multiply these n *remainders in* mod n *arithmetic. Take* $a, b \in \{0, 1, 2, \ldots, n-1\}$*. It may well be the case that* $a+b, a-b$ *or* ab *aren't on this list, but the remainders of this sum, difference and product will be. We may define* mod n *addition, subtraction and multiplication by:*

$$\begin{aligned} a+b &= \textit{remainder when } a+b \textit{ is divided by } n; \\ a-b &= \textit{remainder when } a-b \textit{ is divided by } n; \\ ab &= \textit{remainder when } ab \textit{ is divided by } n. \end{aligned}$$

Notation 126 *We write* $\mathbb{Z}_n$ *for the set of remainders* $\{0, 1, 2, \ldots, n-1\}$ *under the operations of* mod n *arithmetic. Also we will write* mod n *besides a sum, difference or product to denote that we are doing these operations in the context of* mod n *arithmetic.*

Example 127 *In* mod 7 *arithmetic we have*

$$\begin{aligned} 3+6 &= 2 \bmod 7, \ \textit{as } 3+6=9 \textit{ and } 9=1\times 7+2; \\ 3-5 &= 5 \bmod 7 \textit{ as } 3-5=-2 \textit{ and } -2=(-1)\times 7+5; \\ 3\times 5 &= 1 \bmod 7 \textit{ as } 3\times 5=15 \textit{ and } 15=2\times 7+1. \end{aligned}$$

We can more concisely write down all the rules of mod 7 *arithmetic with addition and multiplication tables:*

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Definition 125 has the advantage of being unambiguous (i.e. the operations $+, -, \times$ clearly deliver well-defined answers) but it also looks a little unnatural. For example, is it clear that the distributive law still applies? Alternatively, we can take a more formal view of what the arithmetic of $\mathbb{Z}_n$ is. In Proposition 112, we met the equivalence relation on $\mathbb{Z}$ given by $a \sim b$ if $a-b$ is a multiple of n. We can see now that this is the same as saying

$$a \sim b \ \text{ if and only if } \ a = b \mod n. \tag{4.1}$$

We saw in Example 116 that there are then n equivalence classes $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$. An alternative, more formal but also more natural, definition of the arithmetic of $\mathbb{Z}_n$ is then:

Definition 128 *Let $\mathbb{Z}_n$ denote the equivalence classes $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$ of $\mathbb{Z}$ under the equivalence relation (4.1). We define the operations $+$ and $\times$ on $\mathbb{Z}_n$ by*

$$\bar{a} + \bar{b} = \overline{a+b}, \qquad \bar{a} \times \bar{b} = \overline{a \times b}.$$

Proposition 129 *The operations $+$ and $\times$ are well-defined on $\mathbb{Z}_n$.*

Proof. How might $+$ and $\times$ not be well-defined? Well, because the same equivalence class has many different representatives (e.g. $\bar{1} = \bar{7}$ in $\mathbb{Z}_6$) it's feasible that we might have $\bar{a} = \bar{\alpha}$ and $\bar{b} = \bar{\beta}$ yet $\overline{a+b} \neq \overline{\alpha+\beta}$. Adding the same two elements shouldn't be able to yield two different sums. So suppose that $\bar{a} = \bar{\alpha}$ and $\bar{b} = \bar{\beta}$, then

$$a - \alpha = kn \text{ and } b - \beta = ln$$

for $k, l \in \mathbb{Z}$. But then

$$(a+b) - (\alpha+\beta) = (a-\alpha) + (b-\beta) = (k+l)n$$

and

$$ab - \alpha\beta = (\alpha + kn)(\beta + ln) - \alpha\beta = (k\beta + l\alpha + kln)n$$

and hence $\overline{a+b} = \overline{\alpha+\beta}$ and $\overline{ab} = \overline{\alpha\beta}$ are both true so that $+$ and $\times$ are well-defined. ■

Proposition 130 *(a) $(\mathbb{Z}_n, +)$ is an abelian group isomorphic to C_n.*
(b) Further $\times$ is associative, commutative and distributes over $+$.

Proof. That $(\mathbb{Z}_n, +)$ is an abelian group and the properties of $\times$ mentioned in (b) are all inherited from the same properties in $\mathbb{Z}$. For example, to see that the distributive law still holds, we simply have to note for $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}_n$ that

$$\begin{aligned}
\bar{a}\left(\bar{b} + \bar{c}\right) &= \bar{a}(\overline{b+c}) && [\text{as } + \text{ is well-defined in } \mathbb{Z}_n] \\
&= \overline{a(b+c)} && [\text{as } \times \text{ is well-defined in } \mathbb{Z}_n] \\
&= \overline{ab + ac} && [\text{by the distributive law in } \mathbb{Z}] \\
&= \overline{ab} + \overline{ac} && [\text{as } + \text{ is well-defined in } \mathbb{Z}_n] \\
&= \bar{a}\,\bar{b} + \bar{a}\,\bar{c} && [\text{as } \times \text{ is well-defined in } \mathbb{Z}_n].
\end{aligned}$$

To see that $(\mathbb{Z}_n, +)$ is indeed cyclic we need only note that $\bar{1}$ has (additive) order n. ■

We now note, for certain values of n, that modular arithmetic can have some unfortunate algebraic aspects such as

$$3 \times 5 = 0 \bmod 15, \qquad 4 \times 3 = 0 \bmod 6.$$

It follows that one cannot divide by 3 or 5 in $\mathbb{Z}_{15}$ nor divide by 3 or 4 in $\mathbb{Z}_6$. More generally we note:

Proposition 131 *Let $\bar{x} \in \mathbb{Z}_n$ with $x \neq 0$.*

(a) $\bar{x}$ has a multiplicative inverse if and only if $\mathrm{hcf}(x, n) = 1$. *Hence if n is prime, then $\mathbb{Z}_n$ is in fact a field.*

*(b) Those $\bar{x}$ with a multiplicative inverse (the so-called **units**) form a group $\mathbb{Z}_n^*$ under multiplication.*

Proof. This is left as Exercise Sheet 4, Question 2. ■

Example 132 *List the units in $\mathbb{Z}_{12}$. Identify the group $\mathbb{Z}_{12}^*$.*

Solution. As $12 = 2^2 \times 3$ then the units of $\mathbb{Z}_{12}$ are $1, 5, 7, 11$. Note that the group table is

$*$	1	5	7	11
1	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

showing that $\mathbb{Z}_{12}^*$ is isomorphic to $C_2 \times C_2$. ■

5. ORDER. LAGRANGE'S THEOREM

Recall that we also defined the *order* $\mathrm{o}(g)$ of a group element:

Definition 133 *Let G be a group and $g \in G$. If there is a positive integer k such that $g^k = e$, then the **order** $\mathrm{o}(g)$ of $g \in G$ is defined as*

$$\mathrm{o}(g) = \min\{m > 0 : g^m = e\}.$$

Otherwise we say that the order of g is infinite.

Proposition 134 *If G is finite, then $\mathrm{o}(g)$ is finite for each $g \in G$.*

Proof. Consider the list

$$g, g^2, g^3, g^4, \ldots$$

As G is finite, then this list must have repeats. Hence there are integers $i > j$ such that $g^i = g^j$. So $g^{i-j} = e$ showing that $\{m > 0 : g^m = e\}$ is non-empty and so has a minimal element. ■

Proposition 135 *If $g \in G$ and $\mathrm{o}(g)$ is finite, then $g^n = e$ if and only if $\mathrm{o}(g)|n$.*

Proof. If $n = k\mathrm{o}(g)$ then

$$g^n = \left(g^{\mathrm{o}(g)}\right)^k = e^k = e.$$

Conversely, if $g^n = e$, then there are integers q, r such that $n = q\mathrm{o}(g) + r$ where $0 \leqslant r < \mathrm{o}(g)$. Then

$$g^r = g^{n-q\mathrm{o}(g)} = g^n(g^{\mathrm{o}(g)})^{-q} = e.$$

By the minimality of $\mathrm{o}(g)$ then $r = 0$ and so $n = q\mathrm{o}(g)$. ■

Proposition 136 *If $\phi : G \to H$ is an isomorphism and $g \in G$ then $\mathrm{o}(\phi(g)) = \mathrm{o}(g)$.*

Proof. We have

$$(\phi(g))^k = e_H \iff \phi(g^k) = e_H \iff g^k = e_G$$

as ϕ is injective. ■

Example 137 *In D_8 we have*

$$\mathrm{o}(e) = 1, \quad \mathrm{o}(r^2) = \mathrm{o}(s) = \mathrm{o}(rs) = \mathrm{o}(r^2s) = \mathrm{o}(r^3s) = 2, \quad \mathrm{o}(r) = \mathrm{o}(r^3) = 4.$$

Proposition 138 *Let x, n be integers with $n \geqslant 2$. Then the order $\mathrm{o}(\bar{x})$ of $\bar{x} \in \mathbb{Z}_n$ is*

$$\mathrm{o}(\bar{x}) = \frac{n}{\mathrm{hcf}(x, n)}.$$

Proof. Left to Exercise Sheet 4, Question 1. ■

Corollary 139 *$\bar{x} \in \mathbb{Z}_n$ is a generator if and only if* $\mathrm{hcf}(x, n) = 1$.

Definition 140 *Let H be a subgroup of G.*
*Then the **left cosets** of H (or left H-cosets) are the sets*

$$gH = \{gh : h \in H\}.$$

*The **right cosets** of H (or right H-cosets) are the sets*

$$Hg = \{hg : h \in H\}.$$

Notation 141 *We write G/H for the set of (left) cosets of H in G. The cardinality of G/H is called the **index** of H in G.*

Remark 142 *(i) Note that different elements g_1,$g_2 \in G$ can represent the same (left) coset – i.e we can have $g_1H = g_2H$ yet $g_1 \neq g_2$.*

(ii) In general, we will have $gH \neq Hg$. Obviously we will have $gH = Hg$ if G is abelian, and in other cases as well.

Example 143 *Let $G = S_3$ and $H = \{e, (12)\}$. Then*

$$\begin{aligned} eH = (12)\,H &= \{e, (12)\}; & He = H\,(12) &= \{e, (12)\}; \\ (13)\,H = (132)\,H &= \{(13), (132)\}; & H\,(13) = H\,(123) &= \{(13), (123)\}; \\ (23)\,H = (123)\,H &= \{(23), (123)\}; & H\,(23) = H\,(132) &= \{(23), (132)\}. \end{aligned}$$

Note here that $Hg \neq gH$ in general.

Example 144 *Let $G = S_n$ and $H = A_n$. Then*

$$\sigma A_n = A_n\sigma = A_n \quad \text{when } \sigma \text{ is even;} \qquad \sigma A_n = A_n\sigma = S_n \backslash A_n \quad \text{when } \sigma \text{ is odd.}$$

Note that $\sigma A_n = A_n\sigma$ for all $\sigma \in S_n$, even though S_n is not (in general) abelian.

Example 145 *Let $G = \mathbb{C}^*$ and $H = S^1$. Then, for $w \in \mathbb{C}^*$, we have*

$$wS^1 = \{z \in \mathbb{C}^* : |z| = |w|\}.$$

Example 146 *Let $G = \mathbb{Z}$ and $H = n\mathbb{Z}$. Then the (left and right) coset of $r \in \mathbb{Z}$ is $r + n\mathbb{Z}$. So there are n cosets*

$$0 + n\mathbb{Z}, \quad 1 + n\mathbb{Z}, \quad 2 + n\mathbb{Z}, \quad \ldots \quad (n-1) + n\mathbb{Z} = -1 + n\mathbb{Z}.$$

So we can naturally identity $\mathbb{Z}_n$ with $\mathbb{Z}/n\mathbb{Z}$ (if only as sets for the moment).

Lemma 147 ***(Coset Equality Lemma)*** *Let $H \leqslant G$ and $g, k \in \dot{G}$. Then*

$$gH = kH \iff k^{-1}g \in H.$$

For right cosets, $Hg = Hk \iff kg^{-1} \in H$.

Proof. Suppose that $gH = kH$. Then $g = ge \in kH$ and so there exists $h \in H$ such that $g = kh$. Hence $k^{-1}g = h \in H$.

Conversely suppose that $k^{-1}g = h \in H$. Then $gH = khH \subseteq kH$ and $kH = g\left(g^{-1}k\right)H = gh^{-1}H \subseteq gH$. ■

Remark 148 *The relation on G given by $g \sim k \iff k^{-1}g \in H$ is an equivalence relation on G with the equivalence classes being the left cosets of H. This essentially comprises part of the following proof of Lagrange's Theorem when we prove that the (left) cosets partition G.*

Theorem 149 ***(Lagrange's Theorem)*** *(First instances of theorem due to Lagrange in 1771.)*
Let G be a finite group and H a subgroup of G. Then $|H|$ divides $|G|$.

Remark 150 *There are two steps to this proof. We shall prove:*
(a) The (left or right) cosets of H partition G.
(b) Each (left or right) coset of H is equinumerous with H.
Both (a) and (b) in fact hold for infinite groups.

Proof. Let G be a (not necessarily finite) group G and H a subgroup of G.

(a) For any $g \in G$, note $g = ge \in gH$, so that the union of the (left) cosets is G. Now suppose that two cosets aren't disjoint; we'll show that they must be equal. Say $k \in g_1H \cap g_2H$. Then there are $h_1, h_2 \in H$ such that $k = g_1h_1 = g_2h_2$. Then $g_2^{-1}g_1 = h_1^{-1}h_2 \in H$ and $g_1H = g_2H$ by the Coset Equality Lemma.

(b) For any $g \in G$ then $h \mapsto gh$ is a bijection between H and gH. This map is clearly onto and also 1-1, for if $gh_1 = gh_2$ then we see $h_1 = h_2$ by applying g^{-1}. Hence $|gH| = |H|$.

Finally, if G is finite, then we have

$$|G| = |G/H| \times |H|$$

and hence $|H|$ divides $|G|$. ■

Remark 151 *Lagrange's Theorem states that the order of a subgroup is a factor of the order of the group. The converse does* ***not*** *hold – that is, if G is a finite group and k is a factor of $|G|$ then there need not be a subgroup H of G such that $|H| = k$. For example, $|A_4| = 12$ yet A_4 has no subgroup of order 6. (See Examples 86 and 189.) The converse of Lagrange's Theorem* ***is*** *true for cyclic groups though: for if k divides n then $\overline{n/k}$ has order k in $\mathbb{Z}_n$.*

Example 152 *Find all the subgroups of (i) $\mathbb{Z}_{31}$; (ii) D_{10}; (iii) $\mathbb{Z}_5 \times \mathbb{Z}_5$.*

Solution. (i) As 31 is prime then a subgroup must have order 1 or 31. Hence the only subgroups are $\{\bar{0}\}$ and $\mathbb{Z}_{31}$ itself.

(ii) The subgroups of D_{10} can have order $1, 2, 5$ or 10. So aside from $\{e\}$ and D_{10} we can have order 2 subgroups of the form $\{e,$ reflection$\}$ and the only order 5 subgroup consists of the five rotations.

(iii) $|\mathbb{Z}_5 \times \mathbb{Z}_5| = 25$. So the subgroups can have order $1, 5$ or 25. Every element in $\mathbb{Z}_5 \times \mathbb{Z}_5$ apart from $(\bar{0}, \bar{0})$ has order 5. The subgroups of order 5 consist of the identity $(\bar{0}, \bar{0})$ and four elements of order 5 each of which generate that subgroup. So there are $(25-1)/(5-1) = 6$ such subgroups. Specifically these are

$$\{(\bar{0},\bar{0}),(\bar{1},\bar{0}),(\bar{2},\bar{0}),(\bar{3},\bar{0}),(\bar{4},\bar{0})\}; \qquad \{(\bar{0},\bar{0}),(\bar{0},\bar{1}),(\bar{0},\bar{2}),(\bar{0},\bar{3}),(\bar{0},\bar{4})\};$$
$$\{(\bar{0},\bar{0}),(\bar{1},\bar{1}),(\bar{2},\bar{2}),(\bar{3},\bar{3}),(\bar{4},\bar{4})\}; \qquad \{(\bar{0},\bar{0}),(\bar{1},\bar{2}),(\bar{2},\bar{4}),(\bar{3},\bar{1}),(\bar{4},\bar{3})\};$$
$$\{(\bar{0},\bar{0}),(\bar{2},\bar{1}),(\bar{4},\bar{2}),(\bar{1},\bar{3}),(\bar{3},\bar{4})\}; \qquad \{(\bar{0},\bar{0}),(\bar{1},\bar{4}),(\bar{2},\bar{3}),(\bar{3},\bar{2}),(\bar{4},\bar{1})\}.$$

The only other subgroups are then $\{(\bar{0}, \bar{0})\}$ and $\mathbb{Z}_5 \times \mathbb{Z}_5$. ■

Corollary 153 *Let G be a finite group and $g \in G$. Then $\mathrm{o}(g)$ divides $|G|$.*

Proof. $\langle g \rangle = \{e, g, g^2, \ldots, g^{\mathrm{o}(g)-1}\}$ is a subgroup of G with order $\mathrm{o}(g)$. ■

Remark 154 *This Corollary has no converse: for example, S_3 has no element of order 6. However we shall later prove Cauchy's Theorem which states that if p is a prime factor of $|G|$ then there is a group element with order p. We shall prove this for $p = 2$ (see Corollary 162 below).*

Corollary 155 *Let G be a finite group with $|G| = p$, a prime. Then G is cyclic.*

Proof. Let $g \in G$ with $g \neq e$. Then $\mathrm{o}(g) \neq 1$ and yet $\mathrm{o}(g)$ divides p, so $\mathrm{o}(g) = p$. Hence $|\langle g \rangle| = p$. That is $\langle g \rangle = G$ and G is cyclic. ■

Corollary 156 *Let G be a finite group and $g \in G$. Then $g^{|G|} = e$.*

Proof. $|G|$ is a multiple of $\mathrm{o}(g)$ and $g^{\mathrm{o}(g)} = e$. ■

Theorem 157 ***(Fermat's Little Theorem,** 1640) Let p be a prime and $a \in \mathbb{Z}$ such that p does not divide a. Then $a^{p-1} = 1 \bmod p$.*

Proof. This is just Corollary 156 with $G = \mathbb{Z}_p^*$ as $\left|\mathbb{Z}_p^*\right| = p - 1$. ■

Theorem 158 ***(Euler's Theorem,** 1736) Let $n \geqslant 2$ and let $a \in \mathbb{Z}$ be coprime with n. Then*

$$a^{\phi(n)} = 1 \bmod n$$

where $\phi(n) = |\{k : 0 < k < n, \mathrm{hcf}(k, n) = 1\}|$.

Proof. This is just Corollary 156 with $G = \mathbb{Z}_n^*$ as $\phi(n) = |\mathbb{Z}_n^*|$. ■

Remark 159 *(Off-syllabus) The "phi function" or "totient function" $\phi(n)$ was introduced by Euler in 1760. It is an important number-theoretic function with the following properties.*
(i) $\phi(p) = p - 1$ *for a prime* p.
(ii) $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.
(iii) $\phi(mn) = \phi(m)\phi(n)$ *if* m *and* n *are coprime.*

Lemma 160 *Let* G *be a group. Then the relation* $\sim$ *on* G *defined by*

$$x \sim y \iff x = y \quad or \quad x = y^{-1}$$

is an equivalence relation. The equivalence classes are generally of the form $\bar{x} = \{x, x^{-1}\}$ *unless* x *is self-inverse in which case* $\bar{x} = \{x\}$.

Proof. Left as an exercise. ■

Corollary 161 ***(Wilson's Theorem)*** *If* p *is a prime then*

$$(p-1)! = -1 \mod p.$$

Proof. If $p = 2$ then this just says $1 = -1 \bmod 2$ which is true. So assume $p \geqslant 3$. Consider the self-inverse elements in $\mathbb{Z}_p^*$. We see

$$\bar{x} = \bar{x}^{-1} \iff \bar{x}^2 = 1 \iff (\bar{x} - \bar{1})(\bar{x} + \bar{1}) = \bar{0} \iff \bar{x} = \bar{1} \text{ or } \bar{x} = -\bar{1}$$

as $\mathbb{Z}_p$ is a field. So the only singleton equivalence classes of $\sim$ (the equivalence relation defined in Lemma 160) are $\{\bar{1}\}$ and $\{-\bar{1}\}$ with all others being of the form $\{\bar{x}, \bar{x}^{-1}\}$. As the equivalence classes partition $\mathbb{Z}_p^*$ then

$$(p-1)! = \prod_{\bar{k} \in \mathbb{Z}_p^*} \bar{k} = \prod_{\substack{\text{equivalence} \\ \text{classes}}} \prod_{\substack{\text{each} \\ \text{equivalence} \\ \text{class}}} \bar{k} = \bar{1} \times (-\bar{1}) \times \prod_{\substack{\text{doubleton} \\ \text{equivalence} \\ \text{classes}}} \bar{k} = -\bar{1}$$

as the contribution to the product from each doubleton equivalence class is $\bar{x} \times \bar{x}^{-1} = \bar{1}$. ■

Corollary 162 *Let* G *be a group with even order. Then* G *has an element of order* 2.

Proof. Consider the equivalence relation on G defined in Lemma 160. If there are m doubleton equivalence classes and n singleton equivalence classes, then we have

$$2m + n = |G|$$

as the equivalence classes partition $|G|$. As $|G|$ is even then n is even but we also know $n \geqslant 1$ as e is self-inverse. So, in fact, $n \geqslant 2$ and there is a non-identity element x which satisfies $x = x^{-1}$ or equivalently $x^2 = e$ so that $\mathrm{o}(x) = 2$. ■

Theorem 163 *Let* G *be a finite group with* $|G| = 2p$ *where* $p \geqslant 3$ *is prime. Then* G *is isomorphic to* C_{2p} *or* D_{2p}.

Proof. Assume that G is not cyclic. The possible orders of elements in G are 1 (the identity e) or 2 or p. As $|G| = 2p$ is even then there is an element $x \in G$ of order 2. (Corollary 162). Further if $g^2 = e$ for all $g \in G$ then $G \cong (\mathbb{Z}_2)^n$ for some n (Exercise Sheet 4, Question 5), which is not possible here and hence there is an element $y \in G$ of order p. As x has order 2 and $y, y^2, \ldots, y^{p-1}$ have order p then $x \notin \langle y \rangle$. Hence $G = \langle y \rangle \cup x\langle y \rangle$ or more expansively

$$G = \left\{ e, y, y^2, \ldots, y^{p-1}, x, xy, xy^2, \ldots, xy^{p-1} \right\}.$$

Now the product yx is somewhere amongst G. If $yx = y^i$ we arrive at a similar contradiction to before. So $yx = xy^j$ for some $1 \leqslant j < p$. Then

$$(yx)^2 = yxyx = (yx)\left(xy^j\right) = y^{j+1}; \qquad (yx)^3 = \left(xy^j\right)(yx)^2 = xy^{2j+1};$$

until more generally we find that $(yx)^{2k} = y^{k(j+1)}$ and that $(yx)^{2k+1} = xy^{kj+k+j}$. So yx has an even order and $\mathrm{o}(yx) = 2$. In particular it follows that $j = p - 1$. Hence

$$G = \langle x, y : x^2 = y^p = e, yx = xy^{p-1} \rangle$$

which is a *presentation* for D_{2p}. We can think of x as reflection in a given axis and y as clockwise rotation through $2\pi/p$. ■

Remark 164 *(Off Syllabus)* ***Presentations.*** *Recall that the dihedral group D_{2n} can be defined as*

$$D_{2n} = \langle r, s : r^n = e = s^2, sr = r^{-1}s \rangle. \tag{5.1}$$

Equation (5.1) is an example of a ***presentation*** *for D_{2n}. We can think of r as a rotation and s as a reflection if we want to make real the elements r and s, but there's no great need as the presentation contains everything necessary to describe the algebra of D_{2n} or any group isomorphic to D_{2n}. A presententation of a group describes some* ***generators*** *of the group (here r and s) and the (non-trivial) rules or* ***relations*** *that govern the algebra in the group. Contained in the relations is enough information to show that the group contains $2n$ elements $e, r, , \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s$ and determine products between them. Any other string or* ***word*** *in the generators can be shown to be one of these $2n$ elements by means of the relations. For example, we can see that*

$$sr^3sr^2s = \left(sr^3\right)sr^2s = r^{-3}(ss)r^2s = r^{-1}s = r^{n-1}s.$$

Other group presentations include

$$\mathbb{Z} \cong \langle g \rangle, \qquad C_n \cong \langle g : g^n = e \rangle, \qquad \mathbb{Z}^2 \cong \langle g, h : gh = hg \rangle.$$

There are, of course, many different ways to present the same group. Note $a = s$ and $b = rs$ generate D_6. We can write the other elements as

$$r^2 = ab, \qquad r = ba, \qquad r^2s = aba$$

and see that

$$D_6 = \langle a, b : a^2 = e = b^2, bab = aba \rangle.$$

We need to check we have enough relations. Using the relations $a^2 = e = b^2$ we see that we need only consider those strings (or words) which alternately go a then b. And using the relation $bab = aba$ we can contract substrings of bab from longer words via

$$a(bab) = a(aba) = ba, \qquad (bab)a = (aba)a = ab.$$

The only strings that can't be contracted further in this way are e, a, b, ab, ba, aba.